🔇 КЧОСЕRа

Firmware Upgrade Tool User Guide



Contents

1. Pr	reface	3
1.1	About This Document	
1.2 1.3	About Trade Names	
1.4	About the Firmware Upgrade Tool	
1.5	System Requirements	4
2. Fi	rmware Update	5
2.1	Firmware Update Preparation	5
2.2	Update Product Firmware	5
3. Tr	roubleshooting	14

1. Preface

1.1 About This Document

This document contains a firmware update procedure that uses the "Firmware Upgrade Tool" application software to update the firmware of the product you are using.

1.2 Legal and Safety Information

- Unauthorized copy pf all of part of this guide is prohibited.
- The information in this guide is subject to change without notice.
- This document explains operations using operations performed in Windows 10 as an example.
- We are not responsible for any failures or damages that may occur resulting from conditions or usage procedures not contained in this document.

1.3 About Trade Names

Microsoft, Windows and Windows Server are registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries. All other brands and product names are registered trademarks or trademarks of their respective companies. The designations [™] and [®] will not be used in this guide.

1.4 About the Firmware Upgrade Tool

Firmware is software that controls a product and it is built into the product. By updating the firmware, improvements can be made to the product's security and operations can be stabilized. We recommend using this application to update the product's firmware so that you can continue to use the product safely.

1.5 System Requirements

Operating System:	Windows 8.1, Windows 10,
	Windows 10 Anniversary Update, Windows 11,
	Windows Server 2012, Windows Server 2012 R2, Windows
	Server 2016, Windows Server 2019,
	Windows Server 2022
Memory Capacity:	At least 2 GB
Execution Environment:	Microsoft .NET Framework 4.8 or later
Network:	Wired network connection recommended

2. Firmware Update

Caution

- · A network connection is required during the firmware update.
- The firmware cannot be restored to an earlier version once it has been updated.
- Do not turn off the product or disconnect the network cable during the firmware update. Additionally, the product cannot be used during the firmware update.
- · Make sure that the HTTP/HTTPS port number is not blocked by a firewall or virus scanner.

2.1 Firmware Update Preparation

Perform the following before using this tool to update the firmware.

- Access the support site for your region and download the firmware file to your computer.
- Confirm the setting details of the protocol (SNMPv1/v2c, SNMPv3), and confirm that HTTP and HTTPS is enabled, for the product that is going to have its firmware updated.

Confirm the setting details from Command Center RX. For details, refer to the Command Center RX User Guide.

 Confirm the user name and password for the Administrator that is registered on the product that is going to have its firmware updated.

Note

Confirm the user name and password for the Administrator, not for the Machine Administrator. Refer to the Operation Guide for details on the user name and password for the Administrator.

2.2 Update Product Firmware

- 1. Start up Firmware Upgrade Tool.
- 2. Click [Accept] on the "LICENSE AGREEMENT" screen.

3. Click [Browse], and select the firmware file you downloaded to your computer.

irmware Upgrade Tool		- D >
		续
Firmware file		
File Path	Browse	
Specify the firmware	file	
Devices for upgrad	e	
 Specify IP address 		
Hostname or IP addre	ss	
	Invalid value	
 Local network discove 	ry	
Search for devices usin * Search current doma * Specify IP address ra	ng specified discovery parameters ain ange	
specity in address ta	inge	
Next		

4. Click 🔅.

-		
Firmware Upgrade Tool	-	□ ×
File Path	Browse	
Devices for upgrade		
 Specify IP address 		
Hostname or IP address	Invalid value	
 Local network discovery Search for devices using s Search current domain * Specify IP address range 	specified discovery parameters e	
Next		
	© 2022 KYOCERA Document Solutions Inc.	

5. Set the protocol (SNMPv1/v2c, SNMPv3) information for the product that is going to have its firmware updated.

If SNMPv1/v2c is set to On in Command Center RX

- 1. Select "Use SNMP v1/v2".
- 2. In "Read community," input the SNMPv1/v2c community name.

Firmware Upgrade Tool					- c	
Settings						
SNMP settings						
 Use SNMP v1/v2 						
Read community	public					
 Use SNMP v3 						
User name						
Authentication	Password		Hash	MD5	Ŧ	
Privacy	Password		Encryption	DES	¥	
HTTP/HTTPS settings						
Port number 443						
Last Carat						
Appiy						
	© 2022 KYOCERA Doo	cument Solutions Inc.				

If SNMPv3 is set to On in Command Center RX

- 1. Select "Use SNMP v3".
- 2. In "User Name," input the SNMPv3 user name.
- **3.** If "Authentication" is set to On in Command Center RX, select "Authentication" and input your password, then select the authentication algorithm from the "Hash" dropdown menu.
- If "Privacy" is set to On in Command Center RX, select "Privacy" and input your password, then select the encryption algorithm from the "Encryption" dropdown menu.

immare Upgode tool – Settings SNMP settings O Use SNMP v1/v2 Read community public O Use SNMP v3 User name ∞∞∞∞∞∞∞ ✓ Authentication Password ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	Immare Upgrade Tool Settings SNMP settings Use SNMP v1/v2 Read community User name Authentication Password Privacy Password HTTP/HTTPS settings Port number 443	•••••	Hash MD Encryption DES	- C
Settings SNMP settings Use SNMP v1/v2 Read community public Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Settings SNMP settings Use SNMP v1/v2 Read community public Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	••••••	Hash MD Encryption DES	15 <u> </u>
ettings NMP settings U Se SNMP v1/v2 Read community public Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	ettings NMP settings 0 Use SNMP v1/v2 Read community public 0 Use SNMP v3 User name xcocococo 20 Authentication Password (20 Privacy Password (1110/HTTPS settings 0 ort number 443	••••••	Hash MD Encryption DES	15 v
NMP settings D Use SNMP v1/v2 Read community public User name IZ Authentication Password Privacy Password Encryption DES	NMP settings Use SNMP v1/v2 Read community public Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	•••••	Hash MD Encryption DES	15 ¥
NMP settings 0 Use SNMP v1/v2 Read community public 0 Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	NMP settings Use SNMP v1/v2 Read community Use SNMP v3 User name Authentication Password Privacy Privacy Password TTP/HTTPS settings ort number 443	•••••	Hash MD Encryption DES	15 •)
Use SNMP v1/v2 Read community public Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Use SNMP v1/v2 Read community public Use SNMP v3 user name User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	•••••	Hash MD Encryption DES	15 *
Read community public Use SNMP v3 User name XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Read community public Use SNMP v3 User name Ø Authentication Password Ø Privacy Password TTP/HTTPS settings ort number	•••••	Hash MD Encryption DES	1 <u>5 </u>
Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Use SNMP v3 User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx		Hash MD Encryption DES	15 -
User name xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	User name x00000000 2 Authentication Password 2 Privacy Password ITTP/HTTPS settings ort number 443		Hash MD Encryption DES	15 •]
Authentication Password Hash MD5 Hash MD5 Privacy Password Encryption DES TTP/HTTPS settings ret pumber 443	Authentication Password Privacy Password TTP/HTTPS settings Authentication 443		Hash MD Encryption DES	·5 •
Id Authentication Password Hash (MDS Id Privacy Password Encryption (DES	Introduction Password Privacy Password TTP/HTTPS settings ort number		Encryption DES	• •
Image: C/ Privacy Password Encryption DES TTP/HTPS settings 443	[2] Privacy Password TTP/HTTPS settings ort number 443	******	Encryption DES	
TTP/HTTPS settings	TTP/HTTPS settings ort number 443			· ·
HTTP/HTTPS settings	HTTP/HTTPS settings Port number 443			
TP/HTTPS settings	TP/HTTPS settings tr number 443			
vt number 443	ort number 443			
ort number 443	ort number 443			
	Apply Cancel			
Apply Cancel				

6. (Only when the computer you're using is already using port 443) Specify the HTTP/HTTPS port number.

Note	
Normally, there is no need to change the port number from	ו "443".

Firmware Upgrade Tool				-	ш	×
Settings						
SNMP settings						
 Use SNMP v1/v2 						
Read community	public					
 Use SNMP v3 						
User name						
Authentication	Password	Hash	MD5		Ŧ	
Privacy	Password	Encryption	DES		¥	
HTTP/HTTPS settings Port number 443						
	© 2022 KYOCERA Document Solutions Inc.					

7. Click [Apply].



Click [Cancel] if you want to cancel the change to the settings.

8. Select the product to have its firmware updated.

If specifying the product with an IP address or host name

- 1. Select "Specify IP address".
- 2. Input the product's IP address or host name.

2 Firmware Upgrade Tool	- 🗆 X
	<u>تې</u>
Firmware file	-
File Path Browse	
Devices for upgrade	
● Specify IP address	
Hostname or IP address	
 Local network discovery 	
Search for devices using specified discovery parameters	
* Search current domain * Specify IR address range	
specily in address lange	
Next	
© 2022 KYOCERA Document Solutions Inc.	

3. Click [Next] and proceed to step 9.

If specifying the product by searching for it over the network

1. Select "Local network discovery".

Firmware Upgrade Tool	- 🗆
Firmware file	
File Path Browse	
Devices for unreads	
Devices for upgrade	
 Specify IP address 	
Hostname or IP address	
Invalid value	
Local network discovery	
Search for devices using specified discovery parameters	
* Search current domain	
* Specity IP address range	
Nex	
Not	

2. Click [Next].

- **3.** Do one of the following:
 - If searching from all products on the network, select "Search current domain".
 - If searching from a filtered list of all products on the network, select "Specify IP address range" and input the IP addresses.

Firmware Upgrade Tool			-	×
Local network discover	у			
 Search current domain 				
 Specify IP address range 				
	-			
Invalid value	Invalid value			
Cancel				
	¢	2022 KYOCERA Document Solutions Inc.		

- 4. Click [Next].
- 5. Select the product to have its firmware updated.

Aodel Name	Host name	IP address	Location	
ASKalfa		NUMBER OF		

6. Click [Next].

Note	Note
Click [Retry] to retry the search.	Click [Retry] to retry the search.

9. Click [OK].

Model Name TASKalfa Serial number Host name Paddress Location Immware information Firmware version RNGN RNGN RXCX SPNL OPT ALSPR ALSPR ALEHW	del Name TASKalfa in number tan humber tan h
Serial number Hoat name P address Location Immware type Firmware version New version CPKG ENKM MXX SPNL DPT AL SPR AL SPR	ial number t name ddress ation ware type Firmware version New version GG GS SN XC XC VI. T SFR EHW SI SN SN SN SN SN SN SN
Host name Location Immware Information Immware type Firmware version New version PKG NGN AXX SPNL OPT ALSPR ALSPR ALEHW	st name didness ation mware type Firmware version New version G SN CC L L SN CC L L SN CC L L SN CC L L L L L L L L L L L L L L L L L L
P address Location Immware Information Immware type Firmware version New version CPKG New Version XPXC Second Seco	ddfess ation ware type Firmware version New version G G SN XC U L L SN XC L L L L L L L L L L L L L L L L L L
location irrmware information irrmware version New version PKG NKGN MXXC SPNL OPT AL SPR AL EHW	ation mware tipformation mware type Firmware version G SN K K SN SN SN SN SN SN SN
irmware information Firmware version New version PRG NCM M2XC SPNL OPT AL_SPR AL_EHW	nware information nware type Firmware version New version GN SN SN SN SN SN
Firmware type Firmware version New version PNG NSN M2XC SPNL OPT AL_SPR AL_EHW	nware type Firmware version New version GG SN SX XC U U SPR EHW
CPKG NGN M2XC SPNL DPT AL_SPR AL_ENW	G SN XC VL SR EHW
ENGN MXC SFNL OPT AL_SFR AL_EHW	SN XC 4L 5PR EHW
M2XC SPNL DPT AL_SPR AL_EHW	XC NL T SRR EHW
SPNL OPT ALSPR ALEHW	st T SPR EHW
OPT ALSPR ALEHW	T FR SPR EHW
ALSPR ALEHAW	SPR EHW
ALEHW	HW
Varning	rning
Varning	rning

Caution

Do not turn off the product or disconnect the network cable during the firmware update. Additionally, the product cannot be used during the firmware update.

Note If "WARNING: The device already has a new version installed." is displayed, the

update is unnecessary as the product is already running the newest version of the firmware. Click [Cancel] and end the operation.

10. Input the user name and password for the Administrator registered to the product.

Firmware Upgrade Tool			×
Device information	on		
Property	Value		
Model Name	TASKalfa		
Serial number	To received		
Host name	and approved and a second se		
IP address	10.100.01.01		
Location			
	Authentication		
	Ver must have administrative wirilages to shange device addings. Enter the		
	administrator login and password for the device		
	User name Password		
	Login Cancel		
		_	
Warning			
Read the following info	rmation thoroughly.		
If a device is turned off	or loses power during the upgrade, the device may become inoperable.		
See the user guide for (detailed information.		
Do you want to continu	e with the firmware upgrade?		
bo you mane to contine	a marane mininare apgrade.		
Ca	ncei		
	© 2022 KYOCERA Document Solutions Inc.		

11. Click [Login].

It will start the firmware update.

When the firmware update is finished, "Upgrade completed." will be displayed.

Note

If "Authentication failed. Verify user name and password and try again." is displayed after clicking [Login], there is an error in the user name or password that was entered in step 10. Confirm the correct user name and password.

12. Click [Exit].

3. Troubleshooting

Message	Corrective Actions			
Warning You do not have permission to access this host. Please check your settings and try again. Warning	 Check the host name or IP address you entered is correct. Check the SNMP settings in the [Settings] screen match the protocol settings (SNMPv1/v2c, SNMPv3) on the product. You can check the product protocol settings in Command Center RX. For more information, refer to the Command Center RX User Guide. 			
Devices not found. Search for devices on your local network	 Check the specified firmware file is compatible with your product. 			
Error	 Check the firmware version of the product, and then check the firmware has been updated. 			
Reason: Cannot verify installed version.	(Refer to the Operation Guide for how to check the firmware version of the product.)			
Error	If it has been updated, ignore this error and click [Exit].			
Upgrade failed. Reason: Master file version error	If it has not been updated, check the network is not disconnected and the product is turned on, and then update the firmware again.			
	 If the problem persists, contact your service representative. 			
Error				
Upgrade failed.				
Reason: Cannot write firmware file to device.				